UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/521,827	03/09/2000	Tony M. Brewer	10992150-1	2277

22879 7590 02/23/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
KIANERSI, MITRA	

ART UNIT	PAPER NUMBER
2145	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/521,827	BREWER ET AL.	
	Examiner	Art Unit	
	Mitra Kianersi	2145	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

Applicant's arguments filed 09/22/2004 have been fully considered but they are not persuasive.

Applicant on page 6, line 17, argues that the current action contends that the "data entry" is a record created by the shell program found at column 4 lines 2-9. Using a different "data entry" of Shambroom to meet each limitation involving a "data entry". Thus, Shambroom does not teach all of the claimed limitations. Shambroom on col 7, lines 59-64 teach that once an appropriately secure network connection is established between client 200 and network server 300, server 305 now sends a login form to client 200, and as indicated at 212, client 200, returns login data consisting of the name and password of a Kerberos principal to web server 305. Since the claim language in explaining the limitations of the claim is very broad, the above-mentioned elements thought by Shambroom can be interpreted as "data entry".

Applicant on page 7, line 1 argues that claim 14 recites information tracking the progress of said data operative transaction" the shell program merely records the identity of a user and the date/time of his connection. Shambroom column 4 lines 7-8. This is not information tracking progress of a data operative transaction, but rather is a mere notation that a connection has been established. Thus, Shambroom does not teach all of the claimed limitations. Shambroom in col in col 12, lines 59-67 and col 13, lines 1-19 disclose an Internet Super-Daemon 1280 forks and executes the Secure Remote Execution Daemon 1290, passing command line parameters specifying encryption requirements. The Secure Remote Execution Client 1040 sends the ST for Managed Host 1200 and authenticator #3 to Secure Remote Execution Daemon 1290. The Secure Remote Execution Daemon 1290 extracts the server key for Managed Host 1200 from key table 1310, decrypts the server ticket and sends authenticator #4 to Secure Remote Execution Client 1040, establishing an encrypted connection. Secure Remote Execution Client 1040 then sends command data to Secure Remote Execution Daemon 1290. The Secure Remote Execution Daemon 1290 also extracts access-control lists (ACLs) from ACL file 1330, and verifies that the

Kerberos principal is authorized to execute the command as the specified user on Managed Host 1200. The Secure Remote Execution Daemon 1290 also sends audit trail data (such as, for example, the Kerberos principal name, remote user and host names, local user name, and command data) to System Logging Daemon 1390 on Managed Host 1200. This is to provide a record of all secure remote execution activity. In turn, the System Logging Daemon 1390 can send audit trail data to System Logging Daemon 1400 on Server 700. The System Logging Daemon 1400 records audit trail data in log file 1410.

Applicant on page 7, line 9, argues that claim 20 recites establishing a plurality of data entries related to the progress of said data operative transaction in a destination database." Shambroom teaches that the network server may use client-authenticating information to obtain permission data from the validation center for use in accessing the destination server". The abstract is not different in substance than that of column 7 lines 40-50, and neither describes data entries related to the progress of a data operative transaction. Instead, both relate to acquisition of an encryption key that is used to authenticate access. Shambroom in col 8, lines 1-12 disclose that in FIG. 3 depicts, by way of example only, the process of obtaining client-authenticating information from KDC 400 over an insecure TCP/IP network 350, such as the Internet, that will later be used to establish that network server 300 is acting on behalf of the Kerberos user principal. Other publicly available secure authentication protocols may be used. Implementing an authentication, however, may enhance the security of the system, further protocol that incorporates the use of timestamps. Timestamps can be used to restrict replay attacks, or the recording of some portion of an authentication protocol sequence and use of old messages at a later date to compromise the authentication protocol. Also, Shambroom in col 8, lines 27-41 disclose that using client 200's Kerberos user principal name received at 352, the KDC 400 extracts client 200's secret key from key database 405, which stores secret keys used by KDC 400 and other properly registered clients. Using client 200's secret key, the KDC 400 then encrypts one copy of the KDC session key and creates a permission indicator, which would typically include by way of example only, a timestamp, client 200's user name and

network address, and another copy of the KDC session key. Client will use this permission indicator later 200 to authenticate itself to KDC 400. The permission indicator is encrypted with KDC 400's private key, which is known only to KDC 400; KDC 400, therefore, can later decrypt the permission indicator to verify its authenticity.

Applicant in page 7, line 19, argues that claim 24 recites "a plurality of data entries related to the progress of said memory device control transaction in a destination database". The Abstract teach lines 13-15 as teaching "obtaining data from a destination server". However, at this citation, the Abstract teaches acquisition of "client-authenticating information to obtain permission data from the validation center for use in accessing the destination server," Shambroom Abstract lines 13-15. This citation describes an authentication method of accessing the destination server, but fails to describe data that may be obtained from it. However, even if the Abstract taught "obtaining data from a destination server" as the current action contends, mere "data" possessing no limitation but its source, can not be equated to "data entries related to the progress of said memory device control transaction." Shambroom in col 8, lines 56-67 disclose that in order for client 200 to continue with the transaction, client 200 will have to refresh the memory of server 300. If a hacker or interloper managed to gain access to network server 300 while information was stored in credentials cache 320, only the permission indicator and session key could be obtained, because the Kerberos password is destroyed after being used. This information would be of limited value, however, because the permission indicator, in the preferred embodiment, would contain a date/time stamp and would become worthless after a specified period of time, usually relatively short, has elapsed.

Because the arguments with respect to the allowableness of independent claims were found unpersuasive, these same arguments are not persuasive with respect to the other dependent claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by W.David Shambroom (U.S. Patent number 5,923,756).

1. Regarding independent claim 1, Shambroom teaches a method for executing a transaction in a network having a source site and a destination site, the method comprising the steps of (from a client computer to a destination, abstract, lines1-3)

transmitting an initial transaction request message from source site to destination site;

receiving transaction request message at destination site; (corresponds to a secure connection for receiving and transmitting data is established, abstract, lines 3-5)

generating a data entry related to the progress of data operative transaction in a destination database; (corresponds to generation of additional information which will be used to encrypt future transmissions between client 200 and network server 300. col 7, lines 28-30) and Shambroom on col 7, lines 59-64 teach that once an appropriately secure network connection is established between client 200 and network server 300, server 305 now sends a login form to client 200, and as indicated at 212, client 200, returns login data consisting of the name and password of a Kerberos principal to web server 305. Since the claim language in explaining the limitations of the claim is very

broad, the above-mentioned elements thought by Shambroom can be interpreted as "data entry".

preserving association of data entry with transaction in destination database so long as transaction is active in network (corresponds to the shell program creating records on the network server that maintain a record of the user's identity and use (i.e. time and date). As long as the user is logged on, the shell logon program exists. (The shell program creates records on the network server that maintain a record of the user's identity and use (i.e. time and date). As long as the user is logged on, the shell logon program exists. Col 4, lines 6-9)

2. Regarding claim 2, Shambroom teaches a method comprising the further step of: executing transaction at destination site, thereby producing transaction results (a network server configured as a World Wide Web server creates and executes transient processes (such as when an HTTP Common Gateway Interface (CGI) request is executed) to query the key distribution center. These temporary processes must assume in some sense the identity of the user for the length of the transaction. col 4, lines 13-17).

3. Regarding claim 3, Shambroom teaches a method, where a prospective operation will override transaction results in a memory board (the client user key is a one-way hash of client 200's password and other information, so the network server is able to derive the user key by hashing client 200's password. Both the permission indicator and the KDC session key are stored in credentials cache 320. Web server 305 encodes the contents of the credentials cache 320 and, as indicated at arrow 357, sends the contents of the credentials cache 320 to web browser 205. col 8, lines 46-54) and (credentials cache 830, 5 message is received at destination site (temporarily stored in the credentials cache,col 8, lines 19-30).

4. Regarding claim 4, Shambroom teaches a method of transmitting transaction results to source site over network (col 8, lines 42-44).

5. Regarding claim 5, Shambroom teaches a method of transmitting another transaction request message if no response is received from destination site at source site within a source site time-out period (The security of the system, however, may be

enhanced further by implementing an authentication protocol that incorporates the use of timestamps. Timestamps can be used to restrict replay attacks, or the recording of some portion of an authentication protocol sequence and use of old messages at a later date to compromise the authentication protocol. col 8, lines 7-12) and (col 9, lines 27-28).

6. Regarding claim 6, Shambroom teaches a method deleting initial transaction request message from the network if transaction request message does not reach destination site within a request message time-out period, wherein source site time-out period exceeds request message time-out period to prevent having two transaction request messages simultaneously in transmission through network (the permission indicator, in the preferred embodiment, would contain a date/time stamp and would become worthless after a specified period of time, usually relatively short, has elapsed. col 8, lines 64-67) and (If the time stamp is within the validity period, the KDC 400 generates an access indicator. The access indicator typically would include the Kerberos user principal name, a validity period, and a server session key for use between network server 300 and destination server 500, all of which has been encrypted with the private key of the destination server 500. KDC 400 then sends to network server 300 the encrypted access indicator, and a copy of the server session key encrypted using the KDC session key, as indicated at arrow 362. col 9, lines 27-36).

7. Regarding claim 7, Shambroom teaches a method where upon receiving a duplicate transaction request message, identifying the data entry in the destination database established for transaction, acquiring transaction results; and retransmitting acquired transaction results to source site (Upon receiving a username and password from the user, a host computer compares the password to a list of authorized usernames in an access control file, and if the password matches the password associated with that username, the host computer allows access. col 1, lines 61-66).

8. Regarding claim 8, Shambroom teaches a method, wherein acquiring comprises retrieving transaction results from destination database (In a networked system

comprising multiple interconnected computers, a first computer may request service from a second or destination server through an intermediate server. This first computer is typically called a client. In order to receive service from a destination server, the client must begin by authenticating itself to the destination server. However, because the client may be communicating to the destination server over an insecure line, the client cannot simply send a password in the clear. Instead, the client and the destination server may engage in a multiple query and response exchange, constituting an authentication process, which will convince the destination server that the requesting client is an authorized user. col 2, lines 6-18).

9. Regarding claim 9, Shambroom teaches a method acquiring comprises: executing transaction in response to duplicate transaction request message, thereby producing transaction results (The client-authenticating information is transmitted from the network server to the client and erased from the network server. The client-identifying information is transmitted back to the network server from the client along with a message for the destination server. Permission is obtained to access the destination server from the key distribution center over the insecure network using the secure authentication protocol. At the destination server, the authority of said client to access said destination server is validated using the message. The destination server is accessed with the message if the client's authority is properly validated. col 5, lines 17-24) and (col 14, part 12-b).

10. Regarding claim 10, Shambroom teaches a method of receiving transmitted transaction results at source site; and transmitting, from source site to destination site, a release request to delete data entry associated with transaction in destination database (Web server 305 encodes the contents of the credentials cache 320 and, as indicated at arrow 357, sends the contents of the credentials cache 320 to web browser 205. The authenticating information that may have resided in the network server 300 is then erased or otherwise deleted. Thereafter, in order for client 200 to continue with the transaction, client 200 will have to refresh the memory of server 300. col 8, lines 51-58).

11. Regarding claim 11, Shambroom teaches a method of receiving at destination site, release request to delete data entry associated with transaction; and deleting,

within destination database, data entry associated with transaction, thereby liberating space in destination database. (The web server 720 encrypts the encoded credentials cache and sends the data to the web browser 620, as well as a command form. Once the network server 700 sends the data to the client 600, all transient processes which handled the data exit and terminate and consequently, all authenticating information about client 600 is erased or removed. In order for client 600 to continue with the transaction, client 600 will have to refresh the memory of the server 720 and continue the second phase of the authentication process. col 11, lines 26-35).

12. Regarding claim 12, Shambroom teaches a method of transmitting, from destination site to source site, a release response message, thereby indicating that data entry associated with transaction in destination database has been deleted (col 15, part 16-c).

13. Regarding claim 13, Shambroom teaches a method wherein the source site includes a processor and an agent device, delegating step of transmitting initial transaction request message to agent device. client workstations may be any one of a number of different hardware devices, such as PCs or Macintosh, running a variety of different operating systems, such as UNIX or DOS, and there is no single medium supported by all the varieties of clients. In summary, use of a certificate authentication scheme between the client and the network server would be administratively difficult to support. (col 3, lines 47-51)

14. Regarding independent claim 14, Shambroom discloses a system for reliably executing a transaction at a destination site requested by a source site, the system comprising: (col 2, lines 6-11) and (Abstract, lines 1-3), transmitting an initial transaction request message to destination site from source site; (abstract, lines 3-5), executing a transaction associated with initial transaction request message at destination site; (col 4, lines 13-17), a reservation database at destination site for storing information uniquely identifying and for storing information tracking the progress of data operative transaction (col 4, lines 2-9) and (Shambroom in col in col 12, lines 59-67 and col 13, lines 1-19 disclose an Internet Super-Daemon 1280 forks and executes the Secure

Remote Execution Daemon 1290, passing command line parameters specifying encryption requirements. The Secure Remote Execution Client 1040 sends the ST for Managed Host 1200 and authenticator #3 to Secure Remote Execution Daemon 1290. The Secure Remote Execution Daemon 1290 extracts the server key for Managed Host 1200 from key table 1310, decrypts the server ticket and sends authenticator #4 to Secure Remote Execution Client 1040, establishing an encrypted connection. Secure Remote Execution Client 1040 then sends command data to Secure Remote Execution Daemon 1290. The Secure Remote Execution Daemon 1290 also extracts access-control lists (ACLs) from ACL file 1330, and verifies that the Kerberos principal is authorized to execute the command as the specified user on Managed Host 1200. The Secure Remote Execution Daemon 1290 also sends audit trail data (such as, for example, the Kerberos principal name, remote user and host names, local user name, and command data) to System Logging Daemon 1390 on Managed Host 1200. This is to provide a record of all secure remote execution activity. In turn, the System Logging Daemon 1390 can send audit trail data to System Logging Daemon 1400 on Server 700. The System Logging Daemon 1400 records audit trail data in log file 1410).

15. Regarding claim 15, Shambroom discloses a system, wherein the reservation database is a content addressable memory (col 8, lines 46-50) and (col 11, lines 1-7).

16. Regarding claim 16, Shambroom discloses a system, wherein the source site comprises: a processor (col 3, lines 47-51) and the destination site comprises: a memory (col 8, line 51).

17. Regarding claim 17, Shambroom discloses a system, wherein the source site comprises: a processor agent device for conducting communication with destination site, thereby enabling processor to efficiently concentrate on other tasks (col 3, lines 47-51).

18. Regarding claim 18, Shambroom discloses a system, wherein the source site comprises: a source site database for preserving identification and a status of transaction until transaction is complete (col 8, lines 27-31).

19. Regarding claim 19, Shambroom discloses a system, wherein the processor agent device comprises: a timer for initiating a retransmission of transaction request message if no message responsive to initial transaction request message is received at processor agent device upon expiration of a retransmission time-out period (col 9, lines 18-35).

20. Regarding independent claim 20, Shambroom discloses a system for executing a transaction in a network having a source site and destination site, the system comprising: (abstract, lines 1-3) transmitting an initial transaction request message from source site to destination site; (Abstract 3-5) receiving transaction request: message at destination site; (Abstract, lines 3-5) for establishing a plurality of data entries related to the progress of data operative transaction in a destination database; (abstract, lines 13-15) and preserving data entries with transaction in destination database so long as data operative transaction is active in network (col 9, lines 46-54) and (col 4, lines 2-9) and (Shambroom in col 8, lines 1-12 disclose that in FIG. 3 depicts, by way of example only, the process of obtaining client-authenticating information from KDC 400 over an insecure TCP/IP network 350, such as the Internet, that will later be used to establish that network server 300 is acting on behalf of the Kerberos user principal. Other publicly available secure authentication protocols may be used. Implementing an authentication, however, may enhance the security of the system, further protocol that incorporates the use of timestamps. Timestamps can be used to restrict replay attacks, or the recording of some portion of an authentication protocol sequence and use of old messages at a later date to compromise the authentication protocol. Also, Shambroom in col 8, lines 27-41 disclose that using client 200's Kerberos user principal name received at 352, the KDC 400 extracts client 200's secret key from key database 405, which stores secret keys used by KDC 400 and other properly registered clients. Using client 200's secret key, the KDC 400 then encrypts one copy of the KDC session key and creates a permission indicator, which would typically include by way of example only, a timestamp, client 200's user name and network address, and another copy of the KDC session key. Client will use this permission indicator later 200 to authenticate itself to KDC 400. The permission indicator is encrypted with KDC

400's private key, which is known only to KDC 400; KDC 400, therefore, can later decrypt the permission indicator to verify its authenticity).

21. Regarding claim 21, transactions of a memory read and write. (corresponds to the network server needs to act as if it has the identity and memory of the client server.(col 4, lines 2-4)

22. Claim 22 and 23 recite the same limitation as claim 21. Therefore, they are rejected by the same rationale.

23. Regarding claim 24, a method for executing a memory device control transaction in a network having a source site and a destination site, the method comprising the steps of:

-transmitting an initial transaction request message from source to destination site;(corresponds to integrity and security of messages transmitted from a client to a network server and then to a destination server or from the destination server to a network server and then to the client as part of a distributed computer system.(abstract)

-receiving transaction request message at destination site; (corresponds to establishing a secure connection for receiving data from a client, col18, part [e])

-a plurality of data entries related to the progress of memory device control transaction in a destination database;(corresponds to obtaining data from a destination server, abstract, lines 13-15) and (Shambroom in col 8, lines 56-67 disclose that in order for client 200 to continue with the transaction, client 200 will have to refresh the memory of server 300. If a hacker or interloper managed to gain access to network server 300 while information was stored in credentials cache 320, only the permission indicator and session key could be obtained, because the Kerberos password is destroyed after being used. This information would be of limited value, however, because the permission indicator, in the preferred embodiment, would contain a date/time stamp and would become worthless after a specified period of time, usually relatively short, has elapsed).

-Preserving association of data entry with memory device control transaction in destination database so long as transaction is active in network (corresponds to the shell program creating records on the network server that maintain a record of the user's identity and use (i.e. time and date). As long as the user is logged on, the shell logon program exists. (The shell program creates records on the network server that

maintain a record of the user's identity and use (i.e. time and date). As long as the user is logged on, the shell logon program exists. Col 4, lines 6-9)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mitra Kianersi whose telephone number is (571) 272-3915. The examiner can normally be reached on 8:00AM-4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Valencia Martin Wallace can be reached on (571) 272-6159. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Mitra Kianersi
Feb/10/2005

VALENCIA MARTIN-WALLACE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2700